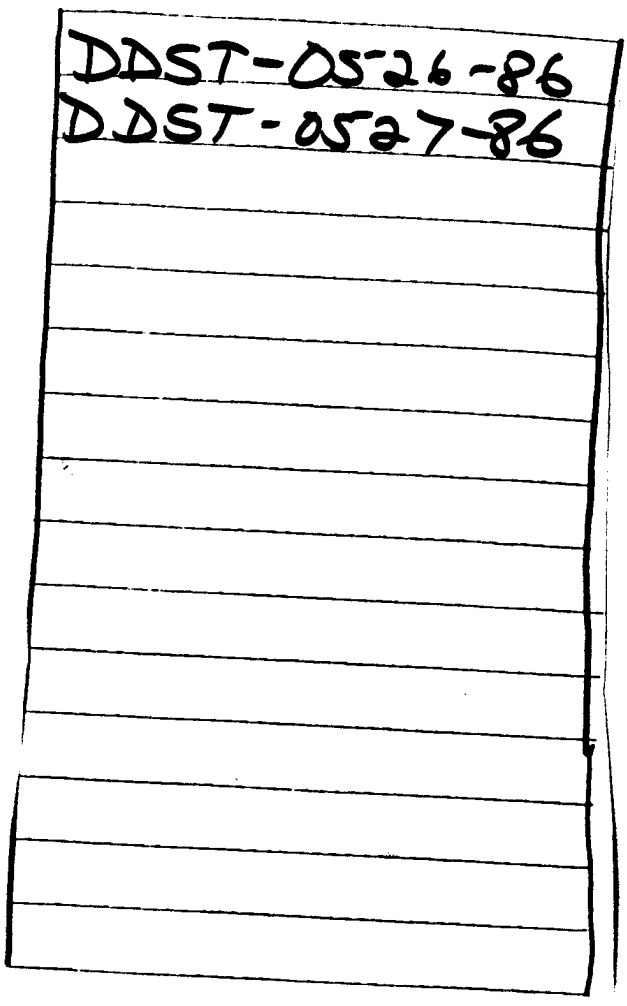
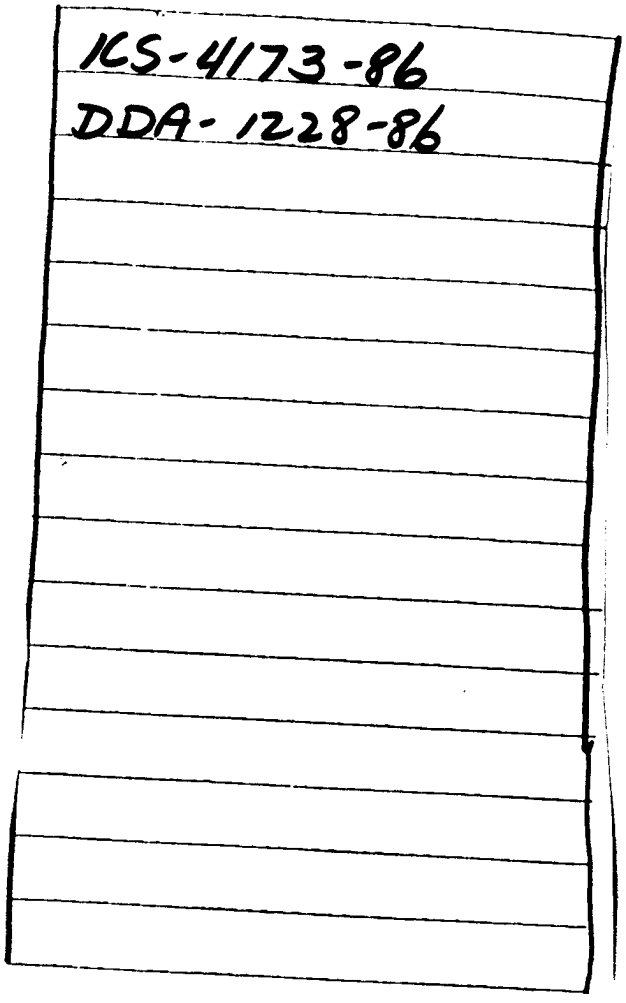
DOCUMENTS CROSS-REFERENCE
ATTACHED: PLEASE TRY NOT TO
REMOVE FROM DOCUMENTS THANKS...



Next 1 Page(s) In Document Denied

DOCUMENTS CROSS-REFERENCE
ATTACHED: PLEASE TRY NOT TO
REMOVE FROM DOCUMENTS THANKS...



STAT

ROUTING AND TRANSMITTAL SLIP

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. Dep. Compt.		
2. 7C 21		
3. HQ		
4.		
5.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

Les,

Per our discussion last week, attached is DDA response to draft unclassified guidance.

[redacted]

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
[redacted]	7D55 HQ
	[redacted]

STAT
STAT

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO : 1980 O - 311-156 (17)

DDA 86-1228
11 July 1986

MEMORANDUM FOR: Chairman, Intelligence Information Handling Committee

FROM: William F. Donnelly
CIA Representative to NTISSC

SUBJECT: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

REFERENCE: Multi-Adse Memo fm Chairman, IIHC, dtd 9 July 1986, Same Subject

1. The draft policy on sensitive information as written is acceptable.

2. Please consider this the response for the Agency. It is written on behalf of the Comptroller and the Executive Director to whom you directed queries.

STAT

William F. Donnelly

ORIG:DDA:WFDonnelly:be
Distribution:
0 - Adse
1 - ER
1 - EA/EXDIR
1 - COMPT
1 - DDA Subj
1 - DDA Chrono

DCI
EXEC
REG

C-204-IR

CR - C-104-IR

Central Intelligence Agency
Washington, D.C. 20505

EA/Executive Director

10 July 1986

Note For: DDA

Bill,

Brenda tells me that you retained your NTISSC hat, so I guess this is yours. Feel free to answer direct.

Let me know if you need any leg work done.

Comptroller received a copy but is bowing out of action.

Would appreciate a copy of whatever goes out.

STAT

STAT

STAT

Next 1 Page(s) In Document Denied

STAT

The Director of Central Intelligence

Washington, D.C. 20505

Intelligence Community Staff

DCI/ICS 86-4173
9 July 1986

MEMORANDUM FOR: See Distribution

FROM: Chairman, Intelligence Information Handling Committee

Subject: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

1. [redacted] asked that we prepare a response on the attached draft policy statement for sensitive, but unclassified information prepared by the National Telecommunications and Information Systems Security Committee (NTISSC) established by NSDD-145. The Systems Security Steering Group, established by NSDD-145 to oversee its implementation, instructed the Chairman of the NTISSC to develop this policy. STAT

2. The draft policy was developed and revised by the subcommittees of the NTISSC in response to recommendations provided by the NTISSC membership. The NTISSC recommended approval of this policy at its last meeting. We would appreciate receiving your comments, including specific recommended changes in line-in, line-out form with supporting rationale, not later than COB 14 July 1986.

STAT [redacted]

Attachment:
Draft Policy on Sensitive Information

UNCLASSIFIED

2

THE WHITE HOUSE

WASHINGTON

July 1, 1986

4668 LOGGED

MEMORANDUM FOR LIEUTENANT GENERAL WILLIAM E. ODOM
National Manager, NTISS

THE HONORABLE DONALD C. LATHAM
Chairman, NTISSC

THE HONORABLE RONALD I. SPIERS
Under Secretary of State for Management

MR. ROBERT M. KIMMITT
General Counsel
Department of Treasury

MR. JOHN N. RICHARDSON
Senior Special Assistant to the
Assistant to the Attorney General
and Chief of Staff
Department of Justice

MR. PHILIP A. DUSAULT
Acting Associate Director
National Security and International Affairs,
OMB

VICE ADMIRAL EDWARD A. BURKHALTER
Director
Intelligence Community Staff

SUBJECT: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

At the first NSDD-145 SSSG Meeting in December, 1985, the Chairman, NTISSC was instructed to prepare a comprehensive policy for the protection of sensitive, but unclassified information handled by Federal Government telecommunications and automated information systems and to leave the determination of what is sensitive to national interests to the heads of Government Departments and Agencies, and entities.

The enclosed draft policy statement for sensitive, but unclassified information prepared by the NTISSC, is forwarded for your review and comment. Request your concurrence and/or comments by July 15, 1986.

Attachment
Tab A Draft Policy

Rodney B. McDaniel
Executive Secretary
National Security Council

3

PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information, will protect that information to the level of threat of exploitation and the associated potential damage to the national interests. The Federal Government is also required to protect those systems which communicate or process personal and financial data provided to it by its citizens as well as company proprietary information while in the possession of U.S. Government Departments and Agencies and entities.

SECTION II - DEFINITION

Sensitive, but unclassified government information is information, the loss, misuse, destruction, or the unauthorized manipulation or alteration of which during its telecommunications or processing via federal government communications or automated information systems, could adversely affect the national interests, citizens, and commercial business of the United States. National interests include, but are not limited to, the wide range of economic, human, financial, industrial, agricultural, technological and law enforcement government information and assets of the United States in addition to national defense and foreign relations matters.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, entities and contractors which electronically transfer, store, process, or communicate sensitive, but unclassified Federal Government information.

SECTION IV - RESPONSIBILITIES

This policy assigns the responsibility to the heads of Federal Government Departments and Agencies for determining what information is sensitive, but unclassified; and for providing systems protection of such information which is electronically communicated, transferred, processed, or stored on government communications and automated information systems.

4

Federal Government Department and Agency heads shall:

a. Determine which of their Department's or Agency's information is sensitive, but unclassified.

b. Identify those categories of information they generate and those categories of information they obtain from the public which warrant protection as sensitive during their communication or processing via government telecommunications or automated information systems. This determination should be based on the Department's or Agency's responsibilities, policies, and experience, and those imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted.

c. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information.

d. Determine in coordination with the National Manager, as appropriate, the threat to and the vulnerability of those identified systems and;

e. Develop, fund and implement a telecommunications and automated information security program, to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

The National Manager shall provide guidance and assistance to Government Departments and Agencies to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.

-

x 5

STAT

STAT

Next 1 Page(s) In Document Denied

STAT

UNCLASSIFIED

The Director of Central Intelligence

Washington, D.C. 20505

Intelligence Community Staff

DCI/ICS 86-4173
9 July 1986

MEMORANDUM FOR: See Distribution

FROM: Chairman, Intelligence Information Handling Committee

Subject: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

1. Vice Admiral Burkhalter asked that we prepare a response on the attached draft policy statement for sensitive, but unclassified information prepared by the National Telecommunications and Information Systems Security Committee (NTISSC) established by NSDD-145. The Systems Security Steering Group, established by NSDD-145 to oversee its implementation, instructed the Chairman of the NTISSC to develop this policy.

2. The draft policy was developed and revised by the subcommittees of the NTISSC in response to recommendations provided by the NTISSC membership. The NTISSC recommended approval of this policy at its last meeting. We would appreciate receiving your comments, including specific recommended changes in line-in, line-out form with supporting rationale, not later than COB 14 July 1986.

STAT

Attachment:
Draft Policy on Sensitive Information

UNCLASSIFIED

2

THE WHITE HOUSE

WASHINGTON

July 1, 1986

MEMORANDUM FOR LIEUTENANT GENERAL WILLIAM E. ODOM
National Manager, NTISS

THE HONORABLE DONALD C. LATHAM
Chairman, NTISSC

THE HONORABLE RONALD I. SPIERS
Under Secretary of State for Management

MR. ROBERT M. KIMMITT
General Counsel
Department of Treasury

MR. JOHN N. RICHARDSON
Senior Special Assistant to the
Assistant to the Attorney General
and Chief of Staff
Department of Justice

MR. PHILIP A. DUSAULT
Acting Associate Director
National Security and International Affairs,
OMB

VICE ADMIRAL EDWARD A. BURKHALTER
Director
Intelligence Community Staff

SUBJECT: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

At the first NSDD-145 SSSG Meeting in December, 1985, the Chairman, NTISSC was instructed to prepare a comprehensive policy for the protection of sensitive, but unclassified information handled by Federal Government telecommunications and automated information systems and to leave the determination of what is sensitive to national interests to the heads of Government Departments and Agencies, and entities.

The enclosed draft policy statement for sensitive, but unclassified information prepared by the NTISSC, is forwarded for your review and comment. Request your concurrence and/or comments by July 15, 1986.

Attachment
Tab A Draft Policy

Rodney B. McDaniel
Executive Secretary
National Security Council

3

PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information, will protect that information to the level of threat of exploitation and the associated potential damage to the national interests. The Federal Government is also required to protect those systems which communicate or process personal and financial data provided to it by its citizens as well as company proprietary information while in the possession of U.S. Government Departments and Agencies and entities.

SECTION II - DEFINITION

Sensitive, but unclassified government information is information, the loss, misuse, destruction, or the unauthorized manipulation or alteration of which during its telecommunications or processing via federal government communications or automated information systems, could adversely affect the national interests, citizens, and commercial business of the United States. National interests include, but are not limited to, the wide range of economic, human, financial, industrial, agricultural, technological and law enforcement government information and assets of the United States in addition to national defense and foreign relations matters.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, entities and contractors which electronically transfer, store, process, or communicate sensitive, but unclassified Federal Government information.

SECTION IV - RESPONSIBILITIES

This policy assigns the responsibility to the heads of Federal Government Departments and Agencies for determining what information is sensitive, but unclassified; and for providing systems protection of such information which is electronically communicated, transferred, processed, or stored on government communications and automated information systems.

4

Federal Government Department and Agency heads shall:

a. Determine which of their Department's or Agency's information is sensitive, but unclassified.

b. Identify those categories of information they generate and those categories of information they obtain from the public which warrant protection as sensitive during their communication or processing via government telecommunications or automated information systems. This determination should be based on the Department's or Agency's responsibilities, policies, and experience, and those imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted.

c. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information.

d. Determine in coordination with the National Manager, as appropriate, the threat to and the vulnerability of those identified systems and;

e. Develop, fund and implement a telecommunications and automated information security program, to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

The National Manager shall provide guidance and assistance to Government Departments and Agencies to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.